WHAT IS CLAIMED IS:

1. A method of monitoring network communications for an indication of an attack and disabling the network communications upon an existence of a predetermined condition, comprising:

monitoring data packets received at a target system in real time;

identifying the received data packets that are associated with signatures of the attack;

determining a severity of the attack; and

blocking the data packets from entering the target system when the severity of the attack exceeds a predetermined threshold.

2. The method according to claim 1, wherein the data packets received at the target system are monitored based on at least one of identifying information and a type of communication.

3. The method according to claim 2, wherein the identifying information includes at least one of an Internet Protocol address and a port number.

4. The method according to claim 2, wherein the type of communication includes at least one of a File Transfer Protocol, a Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, and chat.

5. The method according to claim 1, wherein the data packets received at the target system are monitored using Transmission Control Protocol/Internet Protocol at an application layer.

6. The method according to claim 1, wherein the severity of the attack is determined based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets.

7. The method according to claim 1, wherein the data packets are blocked from entering the target system by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel.

8. The method according to claim 1, further comprising the step of notifying an attacking source of a detection of the attack and of blocking the data packets sent from the attacking source.

9. The method according to claim 1, wherein the data packets are blocked from entering the target system for a predetermined amount of time.

10. A system for protecting a computer network, comprising:

a detection module that receives attack signatures associated with data packets and monitors received data packets for the attack signatures;

a scanning module that evaluates the received data packets having the attack signatures and determines a severity of an attack on the computer network; and

a blocking module that identifies a source of the attack and instructs at least one switching device to block the data packets associated with the attack signatures if the severity of the attack exceeds a predetermined threshold.

11. The system according to claim 10, further comprising a log creating module that is adapted to create a log of the received data packets having the attack signatures.

12. The system according to claim 10, wherein the detection module is adapted to monitor the received data packets based on at least one of identifying information and a type of communication.

13. The system according to claim 10, wherein the scanning module is adapted to determine the severity of the attack based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets.

14. The system according to claim 10, wherein the blocking module blocks data packets from entering the computer network by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel.

15. The system according to claim 14, wherein the blocking module blocks the data packets from entering the network computer for a predetermined amount of time.

16. A computer program product for enabling a computer to monitor received data packets and to disable a transmission medium between a source computer and a destination network upon an existence of a predetermined condition, the computer program product having instructions for enabling the computer to perform operations comprising:

monitoring data packets received at a destination network;

identifying the received data packets that are associated with signatures of an attack;

determining a severity of the attack; and

blocking the data packets from entering the destination network when the severity of the attack exceeds a predetermined threshold.

17. The computer program product according to claim 16, wherein the received data packets are monitored transparently in real-time.

18. The computer program product according to claim 16, wherein the received data packets are monitored after being stored in a storage buffer.

19. The computer program product according to claim 16, wherein the severity of the attack is determined based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets.

20. The computer program product according to claim 16, wherein the data packets are blocked from entering the target system by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel.

21. The computer program product according to claim 16, further comprising the step of notifying an attacking source of a detection of the attack and of blocking the data packets sent from the attacking source.

22. The computer program product according to claim 16, wherein the data packets are blocked from entering the target system for a predetermined amount of time.

23. A computer system configured to monitor data packets received on a transmission medium for an indication of an attack and to block receipt of the data packets upon an existence of a predetermined condition, comprising:

at least one terminal device;

an application server that is coupled to the at least one terminal device for processing requests sent by the at least one terminal device;

a monitoring server that is coupled to the application server for monitoring data packets, the monitoring server having one or more modules comprising:

a first module that receives attack signatures associated with data packets and monitors received data packets for the attack signatures;

a second module that evaluates the received data packets having the attack signatures and determines a severity of an attack on the computer system; and

a third module that identifies a source of the attack and instructs at least one switching device to block the data packets associated with the attack signatures if the severity of the attack exceeds a predetermined threshold.

24. The computer system according to claim 23, wherein the monitoring server further comprises a fourth module that creates a log of the received data packets having the attack signatures.

25. The computer system according to claim 23, further comprising a database coupled to the monitoring server.

26. The computer system according to claim 23, wherein the first module is adapted to monitor the received data packets based on at least one of identifying information and a type of communication.

27. The computer system according to claim 23, wherein the third module is adapted to determine the severity of the attack based on at least one of a frequency

of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets.

28. The computer system according to claim 23, wherein the fourth module blocks data packets from entering the computer network by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel.

29. The computer system according to claim 23, wherein the fourth module blocks the data packets from entering the network computer for a predetermined amount of time.

30. The computer system according to claim 23, wherein the monitoring server issues an alert to inform an administrator of the attack on the computer system.